JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Anti-Theft Security System using Biometric and Mail

Mr. Rohit Takke[1], Miss. Ritu Mane[2], Miss. Karina Rokade[3] , Miss. Sayli Gawade[4],

Dr. (Mrs.) Madhuri Rodge[5]

[1234]BE. Student, Department of Electronics and Telecommunication, Shivajirao S. Jondhle College of Engg. &Technology, Asangaon, Maharashtra. India

[5] Dept. of Electronics and Telecommunication, Shivajirao S. Jondhle College of Engg. &Technology, Asangaon, Maharashtra. India

Abstract: The objective of this project is to create and implement a security system based on fingerprint recognition and GSM/GPRS technology that can be utilized in various settings, such as offices, homes, and banks. The system ensures that only authorized individuals are granted access to secure entry and exit points. Fingerprint recognition and GSM/GPRS technology are utilized in this security system, enabling the lock to open only if the individual scanning their fingerprint is authenticated. Furthermore, when a fingerprint is scanned, the system captures an image of the person, which is then sent to a registered email address. Additionally, a message is sent to a registered mobile number using GSM technology. Email access is facilitated by GPRS technology. In the event that an unauthorized individual attempts to scan their fingerprint, a buzzer will sound, alerting the authorities that an unknown person is attempting to gain access. A photograph of the individual is then captured and sent to the registered email address, and a message is sent to the registered mobile number. Biometric technology and the security system offer numerous benefits over traditional systems. This system can generate a log that records the check-in and check-out times of each user, as well as basic information.

Key Words: Fingerprint, Microcontroller, GSM, GPRS

1.INTRODUCTION

Concerns regarding the safety of their priceless possessions, including jewels, cash, and vital documents, are becoming more widespread in today's culture. In view of this, bank lockers are a popular choice for safeguarding. But consumers have been looking for high-security systems with electronic identification capabilities as rapidly developing technologies have arrived. Intelligent cards, bank lockers, ATMs, user IDs, password-based systems, and more are examples of these determining technologies. Regretfully, hacker attacks, password forgetting, and theft is not always a threat to these systems.

The primary usage of the Global System for Mobile Communication (GSM) is for the transfer and reception of information, including text messaging. Our security system relies heavily on GSM. If someone outside of the authorized user tries to unlock the locker, the user is promptly notified through text message thanks to the usage of GSM. In comparison to conventional approaches, our proposal offers a superior and trustworthy security system via the use of GSM, password, and fingerprint technology-based protection systems. Emails to registered email addresses may additionally be transmitted via General Packet Radio Service (GPRS). GPRS is crucial to our concept since it works with GSM to send an email with the photo of the person who tried to unlock the locker, whether or not they were allowed to.

2. LITREATURE

[1] Literature analysis on fingerprint security system utilizing GSM suggests that this technology is gaining popularity due to its advantages over traditional access control systems. The following are some research that demonstrate the prospects of this technology: Oyewole and Adebiyi's (2017) paper "Design and Implementation of a Fingerprint-Based Security System for ATM Using GSM and GPRS" proposes a system that uses fingerprints to access ATMs. The system transmits data and controls ATM access via GSM and GPRS. The scientists report on extraordinary precision in fingerprint recognition and trustworthy data transmission.

[2] " The paper "Fingerprint Access Monitoring and Control Method Based on GSM and GPRS" by Gao et al. (2018) describes a fingerprint access control system that transmits data and relies on GSM and GPRS for remote monitoring. The system uses fingerprint biometrics for secure access control and is intended for application in compact to medium-sized resources. High accuracy in identification of fingerprints and dependable data transmission are reported by the authors.

[3] Pudukudy and Soman's (2015) work, "A Research Investigation on Fingerprint Authentication System with GSM/GPRS," analyzes how to incorporate GPRS and GSM technologies with fingerprint biometrics for safe access-control applications. High accuracy recognition of fingerprints and dependable data transmission with the recommended system are reported by the authors. A fingerprint identification system that makes use of GSM networks and GPRS methods of transmitting information and remote monitoring is described in "Fingerprint Recognition System Implemented using GSM and GPRS Technology" by Zhang and Hu

(2019).

[4] The research paper "Development of a Biometric Access Management System Employing GSM and GPRS Capabilities" by Abdulqadir and Abdulqadir (2019) describes a fingerprint-based access control system that transmits data and allows for remote monitoring using GSM and GPRS tools. Utilizing fingerprint biometrics, the system offers safe access control and is intended for installation in compact to medium-sized facilities. High accuracy fingerprint identification and dependable data transmission are reported by the authors.

3. PROPOSED SYSTEM

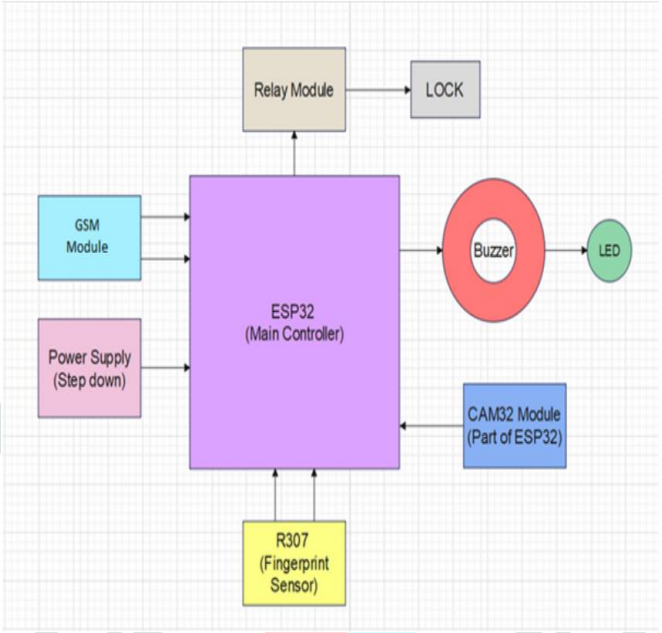


Fig-1*: Block diagram of Anti-Theft Security System Using Biometric & Mail System*

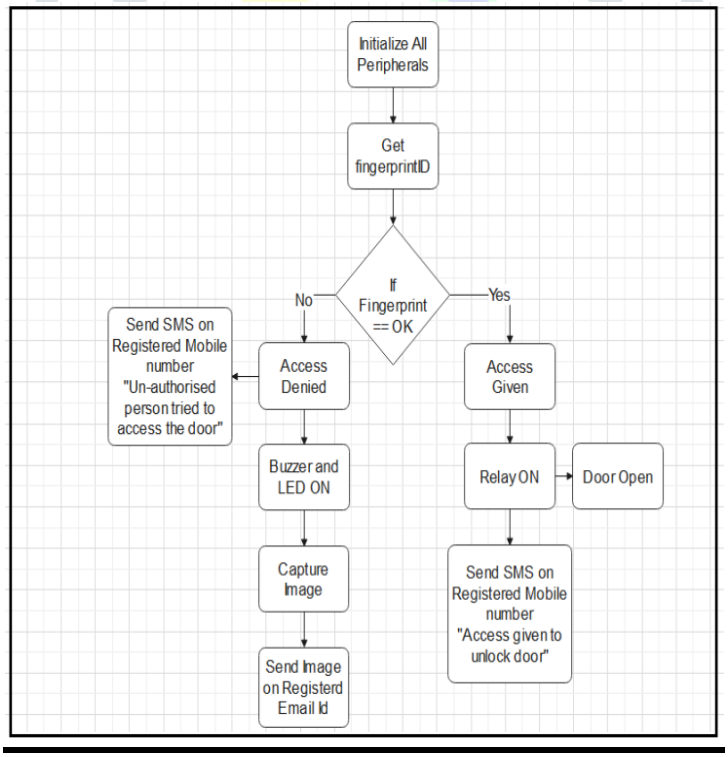


Fig-3: Flow chart of Anti-Theft Security System Using Biometric & Mail System

4. WORKING

A fingerprint-based security system is a type of biometric authentication where access to a device or area is authorized by a person's distinct fingerprint. The way the system operates is that it takes a picture of the user's fingerprint and examines it to see if it fits the authorized user's template that is saved. The general operation of a fingerprint-based security system is as follows:

Initialization: When the power supply has been switched on, the system is turned on and all of the peripherals are initialized. CAM32, ESP32, GPRS, and GSM modules. Enrollment: A fingerprint image of the user is taken and kept in the database of the system. Typically, many fingerprint scans are conducted from various perspectives to get a comprehensive and precise image.

Authentication: The user places their thumb on a scanner that reads fingerprints in order to be granted accessibility to a secured area or device. The fingerprint image is obtained by the scanner, which then compares it to the template that is recorded in the database. Verification: The system allows permission to the user and the GSM module notifies the mobile phone number entered that "Access given for unlocking the door" if the fingerprint collected matches the template that has been stored. Access is refused if the obtained fingerprint does not match. When an unauthorized individual tries to open the door, a buzzer sounds and an LED signal turns on. Additionally, a picture of the individual is taken when the camera module goes on and the buzzer is activated.
The GPRS module is activated and the photograph will be transmitted to the authorized Emil ID as soon as it is taken. Additionally, a message stating that "unauthenticated persons managed to access the door" is sent by the GSM module to the registered cellphone number.
The fingerprint-based security system analyzes each individual fingerprint's distinct characteristics, including ridges, valleys, and minute points, using sophisticated algorithms. Using these characteristics, a computer-generated model of the fingerprint is produced, and its authenticity is checked against a template that has been recorded.

5. RESULT

Using GSM and GPRS for fingerprint security is a very safe and dependable authentication approach that has a number of benefits over more conventional methods. Given the growing significance of the field of cybersecurity, it is a practical way to guarantee that only people with permission can access sensitive systems or gadgets. The results are shown below. The camera records an image and sends it to the authorized email address when someone attempts to get into the system without authorization. The system sends an alert message to the registered mobile number whenever someone attempts to access it, whether they are permitted or not.

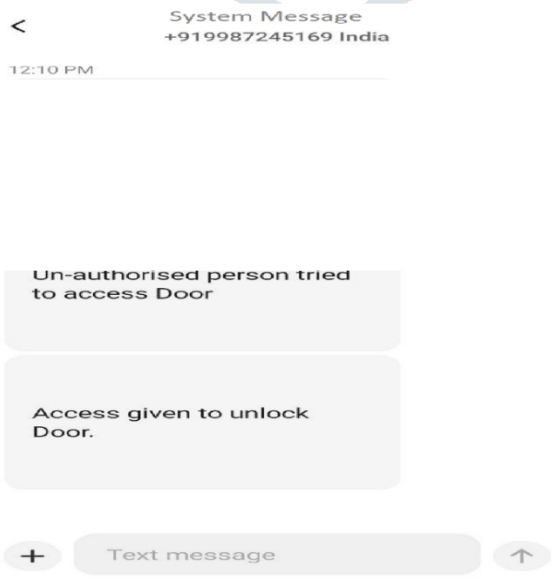
5.1 Unauthorized Biometric Access Attempt:

The biometric authentication procedure would not identify an unauthorized person's biometric information as matching that of an authorized user when they tried to access a secured area or system. Such illegal access attempts ought to be recorded by the security system, which should be configured to record pertinent information such the time, place, and type of attempt.
The unauthorized attempt may cause immediate actions, such as ringing alarms, sending warnings to security staff via the mail system, or turning on video surveillance to capture the occurrence, contingent upon the security policy and the capacity of the system.

5.2 Response and Mitigation:

Security staff can receive instantaneous notifications through the mail system via email or text message upon identifying an attempt at unauthorized access.
Then, depending on how serious the situation is, security officers can take the necessary steps. This could entail looking into the occurrence, remotely shutting down the space or system, or sending someone to handle the situation on-site. Authorities can be alerted for prompt action if the illegal attempt poses an immediate threat.

Fig 4: Screenshot of message sent by system when unauthorized person tries to access



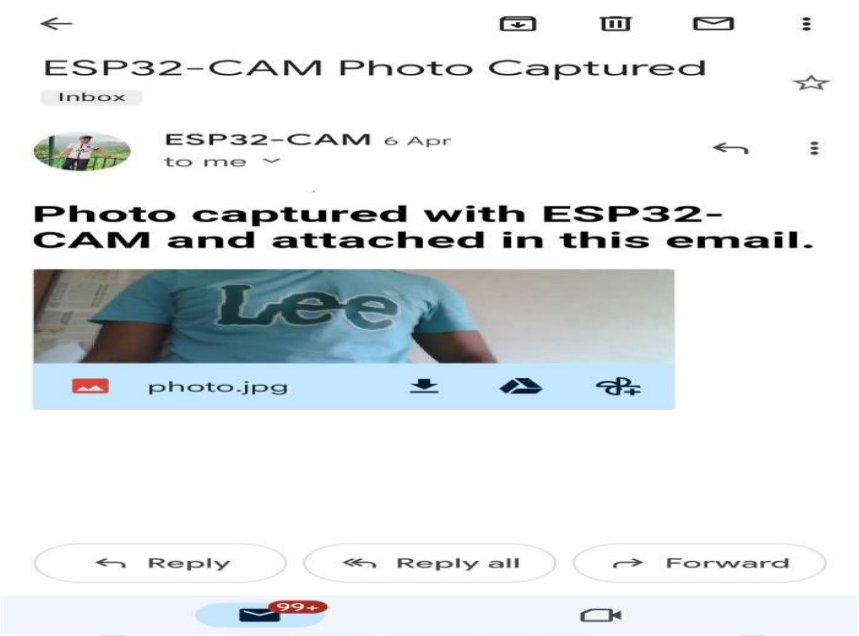


Fig.5: Image captured by CAM32 SMS sent to the Registered Email ID.

5.3 Successful Biometric Authentication:

The authorized individual provides the biometric verification device with their biometric information (facial recognition, iris scanning, fingerprint, etc.). The biometric template linked to the authorized person's identification is saved in the biometric authentication system, which uses it to validate the biometric data that is presented. The authentication procedure is successful if there is a reasonable margin of error between the biometric data and the stored template.

5.4 Permission to Enter:

The authorized individual is granted access by the access control system upon successful biometric authentication. The system or secured area unlocks, granting access to the authorized resources or functionality to the authorized individual.

5.5Notification via Mail System:

The integrated mail system receives a notification from the security system immediately or shortly afterwards the successful authentication. The message notifies the appropriate parties about the effective access attempt, including security administrators and the authorized individual Details like the access time, the authorized user's identity, and any other information thought to be required for security or record-keeping can all be included in the message.

5.6 Continuous Monitoring:

The security system keeps an eye out for any new activities or events in the restricted region or system after the access occurrence. Ongoing security is ensured and any irregularities or suspicious behavior that might arise within the approved person's access timeframe is found through continuous monitoring.

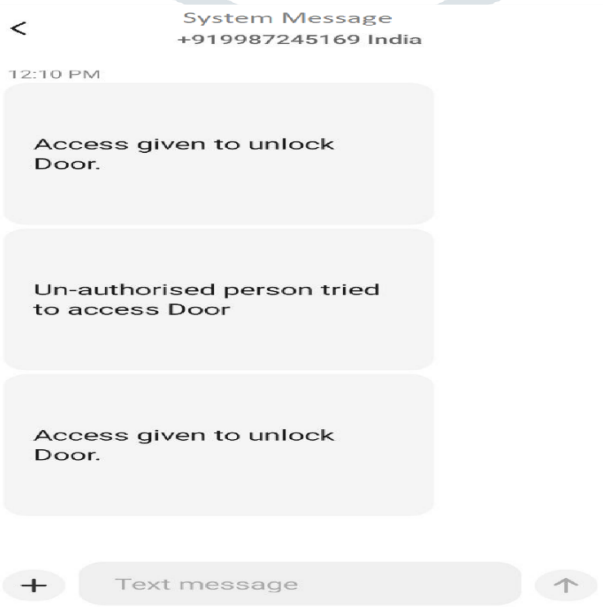


Fig-5: Screenshot of message sent by system when authorized person try to access

6. CONCLUSIONS

To sum up, a finger print-based security system that makes use of GSM and GPRS can function as an efficient and secure method for administrators to handle access and authenticate users. Because the system can authenticate an individual using their fingerprint, it becomes more difficult for unauthorized people to access restricted areas or sensitive data. Furthermore, fast reaction times and remote surveillance have been rendered achievable by the GSM and GPRS techniques' continuous interaction between the scanner that collects fingerprints and the central server.

However, more research is required to ensure the efficacy and security of the system. This research will focus on enhancing the security of interaction channels, optimizing fingerprint recognition algorithms, exploring the integration of other biometric approaches, exploring the possibility of using blockchain technology, and assessing the system's performance in real-world scenarios

REFERENCES

[1] Chaturvedi, S., Kesharwani, S. (2018). A review of biometric authentication using GSM and GPRS technology. International Journal of Computer Applications

[2] Gaur, M. S., Dhaka, V. (2015). Fingerprint recognition based on minutiae extraction and matching using GPRS International Journal of Computer Science and Mobile Computing

[3] Jain, A. K., Ross, A. (2012) Handbook of biometrics Springer US

[4] Kumar, A., Singh, D. (2017) A low-cost fingerprint recognition system using GSM module International Journal of Applied Engineering Research

[5] Nagar, N., Suresh, S. (2018). Fingerprint authentication system using GPRS and Arduino International Journal of Computer Sciences and Engineering

[6] Suthar, M., Patel, S. (2020). A novel approach for fingerprint recognition using GSM and GPRS technology International Journal of Scientific and Technology Research.

BIOGRAPHIES

Mr. Rohit Takke
BE. Student, Department of Electronics and Telecommunication, Shivajirao S. Jondhle College of Engg. &Technology, Asangaon, Maharashtra,India

Miss. Ritu Mane
BE. Student, Department of Electronics and Telecommunication, Shivajirao S. Jondhle College of Engg. &Technology, Asangaon, Maharashtra, India

Miss. Karina Rokade
BE. Student, Department of Electronics and Telecommunication, Shivajirao S. Jondhle College of Engg. &Technology, Asangaon, Maharashtra,India

Miss. Sayli Gawade
BE. Student, Department of Electronics and Telecommunication, Shivajirao S. Jondhle College of Engg. &Technology, Asangaon, Maharashtra,India

Dr. (Mrs.) Madhuri Rodge,
Head of Dept. of Electronics and Telecommunication,
Shivajirao S. Jondhle College of Engg. &Technology, Asangaon,
Maharashtra. India